UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/039,595	12/31/2001	Andrew F. Glew	42390.P13735	2224

7590   09/18/2006

John P. Ward, Esq.
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER
FIELDS, COURTNEY D

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/039,595	GLEW ET AL.
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *10 July 2006*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-20* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claim 11 has been amended.

2.   Claims 1-20 are pending.

Response to Arguments

3.   Applicant's arguments with respect to claim 1 have been considered but are moot

in view of the new ground(s) of rejection, Wong (Pub No. 2002/0150252)

Claim Rejections - 35 USC § 101

4.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
> matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
> conditions and requirements of this title.

5.   Claims 1 and 19 are rejected under 35 U.S.C. 101 because the claimed invention

is directed to non-statutory subject matter. Claims 1 and 19 are not limited to tangible

embodiments. In view of Applicant's disclosure, specification page 7, lines 5-17, page

13, lines 2-5 and page 11, lines 13-21. With regards to claim 1, the code module and

the machine readable medium is not limited to tangible embodiments, instead being

defined as including both tangible embodiments (i.e. disk or memory storage device)

and intangible embodiments (i.e., software program per se). A computer program is

merely a set of instructions capable of being executed by a computer, the computer

program itself is not a process. Computer programs do not define any structural and

functional interrelationships between the computer program and other claimed elements

of a computer which permit the computer program's functionality to be realized. When

nonfunctional descriptive material is recorded on some computer-readable or machine-

readable medium, in a computer, on a data structure, or on an electromagnetic carrier

signal, it is not statutory. As such, claims 1 and 19 are not limited to statutory subject

matter and is therefore non-statutory.

6.   A computer program per se and a machine-readable medium stored on a data

structure do not fall within one of the four statutory categories of the invention, (i.e.,

process, machine, compositions of matter, and manufacture).

Claim Rejections - 35 USC § 112

7.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

8.   Claims 1 and 19 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

9.   Claims 1 and 19 provides for the use of code to be executed and decrypting the

signature using a key embedded in a chipset, but, since the claim does not set forth any

steps involved in the method/process, it is unclear what method/process applicant is

intending to encompass. A claim is indefinite where it merely recites a use without any

active, positive steps delimiting how this use is actually practiced.

        Claims 1 and 19 are rejected under 35 U.S.C. 101 because the claimed recitation

of a use, without setting forth any steps involved in the process, results in an improper

definition of a process, i.e., results in a claim which is not a proper process claim under

35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and

Clinical Products, Ltd. v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

        Appropriate correction is required.

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

11.   Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Davis et al. (US Patent No. 6,401,208) in view of Wong (Pub No. 2002/0150252).

Referring to the rejection of claims 1 and 11, Davis et al. teaches and discloses a

technique for verifying if the BIOS code has been illicitly modified, by using a pre-

programming cryptographic device. The cryptographic device contains BIOS code, a

BIOS certificate and a BIOS signature. The BIOS signature is decrypted with the

certificate key. BIOS signature is retrieved from the BIOS cryptographic device by

decrypting the BIOS certificate using a root certification key, retrieving a public key from

the BIOS signature and using the public key to recover a pre-loaded digest. (See

Column 5, lines 4-67, Column 6, lines 1-13)

However, Davis et al. does not teach decrypting the signature using a key

embedded in a chipset of the computing device.

Wong teaches and discloses a decryption key circuit used for the IP provider

wherein the computing device is capable of decrypting the configuration code using an

embedded decryption key located within the FPGA (chipset) of the computing device.

(See Wong, page 3, Section 0031)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Davis et al.'s method for authenticating BIOS code with Wong's integrated circuit decryption circuit. Motivation for such an implementation would enable a better way of securing the configuration of IP of an FPGA user by embedding the ASIC with a decryption key circuit. The embedded decryption key may be used to by an IP provider to help configure the integrated circuit. (See Wong, page 1, Sections 0007-0008)

Referring to the rejection of claims 2 and 12, (Davis et al. as modified) discloses the claimed limitation wherein the signature further attests to the authenticity of the data (See Column 2, lines 64-66)

Referring to the rejection of claims 3, (Davis et al. as modified) discloses the claimed limitation wherein the signature comprises a digest value computed from the code and the data (See Column 2,lines 56-61)

Referring to the rejection of claims 4,13, and 20, (Davis et al. as modified) discloses the claimed limitation wherein after recovering a pre-loaded digest, the BIOS code undergoes a one-way hash (SHA -1 hash) function to produce a resultant digest. If there is a match, the BIOS code becomes authenticated. (See Column 5, lines 66-67, Column 6, lines 1-19) The one-way hash derives from the Digital Signature Standard, which converts the information of a variable-length into information of a fixed length (i.e., digest) (See Column 2, lines 46-64)

Referring to the rejection of claims 5, (Davis et al. as modified) discloses the claimed limitation wherein the signature comprises a hash of the code and the data (See Column 2, lines 53-67, Column 6, line 1)

Referring to the rejection of claims 6 and 14, (Davis et al. as modified) discloses the claimed limitation wherein identifying when execution of BIOS code should be prevented or accessible by authenticating BIOS code using a cryptographic device as a means for computing. (See Column 5, lines 9-32)

Referring to the rejection of claims 7 and 15, (Davis et al. as modified) discloses the claimed limitation wherein once the BIOS code has been authenticated, the cryptographic device generates a predetermined signal (marker) of code, in order to begin and end execution. Once the instructions have been fetched to the vector, the BIOS code becomes authenticated. (See Column 6, lines 20-30) As defined in the Applicant's Specification, on page 13, lines 9-12, a marker comprising a predefined bit pattern that signals the end of the code pages and data pages. Therefore, the predetermined signal is equivalent to the marker of code.

Referring to the rejection of claims 8 and 16, (Davis et al. as modified) discloses the claimed limitation wherein the cryptographic engine which performs encryption and decryption as DES-based or RSA based (i.e., encryption algorithms). The chipset contains code modules such as BIOS code for performing cryptographic functions within the IC devices (See Column 3, lines 31-40, Column 4, lines 21-40)

Referring to the rejection of claims 9 and 17, (Davis et al. as modified) discloses the claimed limitation wherein a field that specifies an execution point of a post-code

module from which the computing device initiates execution of the post-code module

after executing the code module (See Column 5, lines 4-31)

Referring to the rejection of claims 10 and 18, (Davis et al. as modified) discloses

the claimed limitation wherein the code comprises a terminate instruction that specifies

an execution point of a post code module and that in response to being executed results

in the computing device terminating execution of the code module and initiating

execution of the post-code module from the execution point (See Column 5, lines 32-67,

Column 6, lines 1-13)

Referring to the rejection of claim 19, (Davis et al. as modified) discloses a

machine readable medium comprising: data pages comprising data, code pages

comprising code to be executed by a computing device and a value that fingerprints the

data pages and the code pages,(See Column 5, lines 66-67, Column 6, lines 1-13)

However, Davis et al. does not teach decrypting the value using an asymmetric

key embedded in a hardware component of the computing device.

Wong teaches and discloses a decryption key circuit used for the IP provider

wherein the computing device is capable of decrypting the configuration code using an

embedded decryption key located within the FPGA (chipset) of the computing device.

(See Wong, page 3, Section 0031)

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to combine Davis et al.'s method for authenticating BIOS

code with Wong's integrated circuit decryption circuit. Motivation for such an

implementation would enable a better way of securing the configuration of IP of an

FPGA user by embedding the ASIC with a decryption key circuit. The embedded
decryption key may be used to by an IP provider to help configure the integrated circuit.
(See Wong, page 1, Sections 0007-0008)

Regarding claim 20, (Davis et al. as modified) discloses the claimed limitation
wherein the value is encrypted via the RSA encryption algorithm and an asymmetric key
paired with the asymmetric key of the hardware component and the value comprises a
SHA-1 hash of the data pages and the code pages (See Column 4, lines 29-40)

Conclusion

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Courtney D. Fields whose telephone number is 571-
272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off
every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number
for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
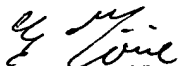Business Center (EBC) at 866-217-9197 (toll-free).

cdf

September 12, 2006

EMMANUEL L. MOISE

SUPERVISORY PATENT EXAMINER